Sills Cummis & Gross
A Professional Corporation
101 Park Avenue, 28th Floor
New York, New York 10178
Tel: (212) 643-7000
Fax (212) 643-6500

The Legal Center
One Riverfront Plaza
Newark, NJ 07102
Tel: (973) 643-7000
Fax: (973) 643-6500

Joseph B. Shumofsky
Member
Admitted In NJ, NY
Direct Dial: 973-643-5382
Email:
jshumofsky@sillscummis.com

222 Lakeview Avenue, Suite 800
West Palm Beach, FL 33401
Tel: (561) 693-0440
Fax: (561) 828-0142

December 4, 2024

VIA ECF
Honorable Michael A. Hammer
United States District Court
Martin Luther King Building & U.S. Courthouse
50 Walnut Street
Newark, NJ 07101

Re: ***Nina Agdal v. Dillon Danis*, 23-CV-16873 (MCA)(MAH)**

Dear Judge Hammer:

We represent Plaintiff Nina Agdal. We write to apprise the Court that an independent forensic specialist conducted an initial inspection of Defendant Dillon Danis's dead cellular phone and determined it is very likely its condition is the result of an *intentional* effort to render it inoperable and, thus, destroy electronically stored information (ESI) central to this case. We therefore request that, as a precursor to a motion for spoliation sanctions under Fed. R. Civ. P. 37, the Court order Defendant to pay the expenses associated with completing a forensic examination of the phone in order to confirm whether the data thereon is unrecoverable, as appears to be the case. Plaintiff already incurred over $5,000 in forensic expenses, and, under the circumstances, it would be unjust for Plaintiff to bear the additional expenses.

The Court is aware of the history of Defendant's discovery misconduct, which has frustrated the prosecution of this case. Defendant's cellular phone was the exclusive device he used during the period at issue to post about Plaintiff and search for content of her to post. Third-party discovery revealed that he also used the phone to text with others about his harassing conduct and to coordinate future posts about Plaintiff, despite denying under oath that he had done so in his interrogatory answers. The phone and its contents are thus crucial to this case. In August 2024, after Plaintiff's repeated requests for text messages and other ESI from the phone, and after several Court orders instructing Defendant to provide those materials (including at an in-person show cause hearing in July 2024), Defendant informed Plaintiff and the Court for the first time that the phone had purportedly "died" in January 2024 and that, as a result, he could not access all of the data on the phone (only select images that had been backed up to the cloud). Defendant eventually turned the dead phone over to his counsel, who then provided it to us, but only after Defendant had ignored several more Court orders between August and October and made Plaintiff incur additional expense in chasing him for it. Upon receiving the phone, we provided it to a forensic specialist (Erik Rasmussen of Grobstein Teeple LLP) for analysis.

Pursuant to Court order, in October, we also deposed Defendant related to his discovery efforts, specifically with respect to circumstances surrounding the dead phone and his preservation efforts. At his deposition, Defendant was unable to offer a credible account regarding the loss of the data on his phone (*i.e.*, how his phone "died") or a reasonable explanation for why the data had not been preserved at the outset of this case, considering a party's independent obligation to preserve all relevant data. Based on an initial assessment of the

phone, Mr. Rasmussen confirmed that the charging port on the phone has been rendered inoperable and the phone will not turn on. Notably, Mr. Rasmussen is of the opinion that Defendant's testimony regarding the condition of the phone—that the device died after he took it in the sauna and then subsequently tried to charge it—is contradicted by the design features of this particular model of phone (the Apple iPhone 14 Pro Max) and a physical inspection of the phone's condition. Exhibit A, Rasmussen Decl. at ¶¶ 8–11. In other words, our expert indicates it appears highly likely that Defendant is lying about how his phone was damaged.

The potentially spoliated data is unquestionably relevant to the claims and defenses here. Mr. Rasmussen believes there are additional measures he can attempt to try and repair the damaged components of the phone to turn on, to then try and determine conclusively whether the data on the phone is irretrievable. He also believes that, in the event the phone is successfully restored, the data logs may also provide some information about what led to its incapacitation. Mr. Rasmussen estimates these efforts would cost up to $5,000 for the initial next steps of trying to restore the phone to power on and then, if those efforts are successful, between $16,200 to $23,500 in additional fees to extract any data that is recoverable. *Id.* at ¶¶ 17–18.

The continued forensic examination would definitively answer whether the subject ESI is recoverable and is a precursor to bringing a motion for spoliation sanctions under Rule 37. Accordingly, given the necessity of this step, Defendant's obstruction in discovery to date, Defendant's culpability in causing the incapacitation of the phone (which an initial assessment determined was likely intentional), and the fact that Plaintiff has already incurred over $5,000 in forensic expenses relating to Defendant's phone, we ask that the Court order Defendant to pay

for the costs of the forensic examination. *See, e.g.*, *AMG Nat'l Tr. Bank v. Ries*, 2011 WL 3099629, at *5 (E.D. Pa. July 22, 2011) (ordering the defendant to pay the costs of a forensic examination of his computer, when the evidence "strongly suggest[ed] that his purpose in deleting the files was to prevent their discovery"); *ShowCoat Sols., LLC v. Butler*, 2019 WL 3332617, at *5 (M.D. Ala. June 7, 2019), *R&R adopted*, 2019 WL 3560081 (M.D. Ala. Aug. 5, 2019) (ordering, as an initial step, that defendants pay the costs of a forensic examination concerning a cell phone defendants had destroyed); *TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo*, 2017 WL 1155743, at *2 (D.P.R. Mar. 27, 2017) (ordering defendant to pay for a forensic examination of a hard drive, when evidence showed defendant had attempted to intentionally spoliate data from the hard drive and other electronic devices).

The Defendant's Position[1]

Defendant opposes Plaintiff's attempt to impose upon him the expense of Plaintiff's own forensic fishing expedition. This lawsuit is about the posting of a photograph on Twitter that, discovery in this case has established, was taken by Plaintiff's former boyfriend and subsequently made available on the internet, along with a multitude of other nude photographs of Plaintiff, who earns her living by posing in state of partial and complete undress. In her complaint, Plaintiff also references material posted by Defendant that had allegedly been hacked from her account. Plaintiff has been provided in discovery a third-party Twitter post of some of that content which predates Defendant's post of the content. Discovery also has established that

[1] Pursuant to this Court's prior Order (D.E. 68), requiring any discovery disputes to be presented to the Court in a joint letter, we solicited Defendant's position regarding Plaintiff's requests and included it here.

Defendant's primary means of communication was via messaging (not email or text), and Plaintiff has received all of Defendant's Twitter, What's App and Facebook messaging. Plaintiff also has obtained texts from third parties, none of which suggest that there is a horde of relevant texts that Plaintiff has not received or which were destroyed.

There is no evidence that there is any material of substantial value on Defendant's non-functioning mobile telephone. Therefore, at least in the first instance, Plaintiff should continue to incur the expense of any additional forensic examination of the mobile telephone. A spoliation motion, or request to shift costs to Defendant, is entirely premature.

* * *

Thank You for the Court's consideration of this matter.

Respectfully submitted,

SILLS CUMMIS & GROSS, P.C.
/s/ Joseph B. Shumofsky
Joseph B. Shumofsky, Esq.

MARCUS NEIMAN
RASHBAUM & PINEIRO LLP
/s/ Jeffrey A. Neiman
Jeffrey A. Neiman, Esq.
Jason L. Mays, Esq.

Encl.
cc: Counsel for Defendant Dillon Danis (via ECF)

Exhibit A

UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

NINA AGDAL, v. DILLON DANIS.	Case No.: 2:23-cv-16873 **DECLARATION OF ERIK RASMUSSEN**

I, Erik Rasmussen, declare as follows:

1. In November 2024, I was engaged by Nina Agdal, whom I understand is the Plaintiff in this case, to examine an Apple iPhone 14 Pro Max. I am informed that the iPhone belonged to Dillon Danis, the Defendant in the case. I have also reviewed Mr. Danis's testimony about the circumstances in which he claims his phone died—specifically, his testimony that he had taken the phone in the sauna with him, and that he was no longer able to charge the phone or get it to turn on after that point.[1]

2. I provide this Declaration for two purposes: *First*, to provide my professional opinion that there is a high likelihood that Mr. Danis's phone was intentionally damaged (*i.e.*, and not damaged in the manner described by Mr. Danis). And *second*, to explain the initial steps I took in inspecting the phone and attempting unsuccessfully to get it to turn on, and to provide an estimated cost for next steps in attempting to repair the phone and determine whether any data is recoverable.

Credentials

3. I am the Global Head of Cybersecurity and Risk Management Solutions at the consulting firm Grobstein Teeple LLP, headquartered in Woodland Hills, California. I am also

[1] Mr. Danis also testified the phone may have been an iPhone 15, which uses a different charging cable than the phone I examined, but for purposes of this Declaration, the distinction between the different models it not pertinent as my analysis would be functionally the same.

the Chief Executive Officer of Total Executive Security LLC, also headquartered in Woodland Hills, California. My curriculum vitae is attached hereto as **Exhibit 1**.

4. My background includes over eighteen years in cybersecurity with a particular emphasis on digital forensics of various computer systems and mobile devices, including Apple devices such as MacBooks, iPads, and iPhones. I have consulted on cybersecurity-related matters for a broad range of clients, including both individuals and public and private entities (e.g., startups, non-profits, health care companies, municipalities, private corporations, and educational institutions).

5. I spent nearly two years as a deputy prosecuting attorney in Washington State and over nine years as a Special Agent with the United States Secret Service, where I was a member of the Electronic Crimes Special Agent Program ("ESCAP") specializing in data breach investigations and extensive digital forensics on devices. My assignments also included two years at Headquarters assigned to the Cyber Intelligence Section ("CIS"). My work included forensic analysis of devices seized during the investigation of transnational cybercrime, to include Apple devices, as well as testifying under oath to my findings and drafting affidavits reviewed and approved in both federal and state court.

6. Following my government service, I worked for Fidelity National Information Services (aka "FIS Global"), an international financial technology company and Visa Inc., the world's largest payment card brand. Both positions included digital forensics or review of report of findings for major data breaches against merchant computer networks where digital forensics were conducted. I have also consulted for nearly eight years in various capacities for cyber advisory services, to include testifying as an expert witness in alternative dispute resolution ("ADR") cases, and in both federal and state court, where forensic examination of mobile devices, specifically Apple mobile devices, were at issue.

Likelihood of Intentional Damage to iPhone

8. When I received Mr. Danis's Apple iPhone 14 Pro Max, I first attempted to charge the phone with a standard lightning cable connector. The phone would not charge and therefore could not be powered on. I physically inspected the phone's exterior but did not observe any obvious signs of tampering. For example, there were no bent pins in the lightning connector port, nor were there scratch marks indicative of a foreign object being placed in the port. The screen was intact, as were the buttons on the side of the phone.

9. Once I removed the screen, however, there was corrosion in the interior on the lightning connector assembly. This is significant because of the extreme conditions that an iPhone 14 Pro Max must be subjected to in order for such corrosion to occur.

10. This model of iPhone has what is called an "Ingress Protection" rating of IP68, which in relevant part means that the device is designed to stay operational even if it is submerged in water for up to 30 minutes at a depth of several meters.[2] Moisture accumulation or high humidity from having the phone in a sauna could damage internal components, to include the battery, but there was no visible damage to the battery. Moreover, unless the battery is damaged, plugging a charging cable into this model of iPhone should have still prompted a liquid detection alert on the screen, instructing the user to let the phone dry. Mr. Danis did not testify to seeing any kind of alert. In any event I do not recall a scenario in which an iPhone was "fried," or a charging port damaged beyond use, as a result of sauna conditions.[3]

---

[2] The first numeral of the rating is tied to foreign object/dust related testing, while the second numeral is tied to water testing. Nine (9) is the highest numeral the rating system uses for water, which provides some indication for just how much water and moisture this model of phone is able to withstand.

[3] Moreover, Mr. Danis testified that he regularly he used the iPhone in the sauna, suggesting a familiarity with the potential impact moisture could have on his phone, especially if it was charged after exposure to the sauna. Again, this would likely trigger alerts on the phone, which did not appear to happen here. Also, based on my training and experience with mobile device forensics generally, if

11. Based on my experience and the condition of the phone, I do not find Mr. Danis's explanation of what happened to his phone to be plausible. Instead, I believe it is highly likely that intentional water damage occurred here, because the presence of corrosion (even after a period of time has passed whereby the device has "dried" out) indicates that the device was exposed to water for a significant period and/or depth greater than what the phone was designed to withstand.

12. After observing the corrosion on the iPhone, I installed a new lightning connector assembly, used different charging cables, and replaced the battery, but these steps were unsuccessful in restoring the functionality of the charging port.

13. It is possible that through additional efforts, we might be able to get the phone to turn on via a charging cable and to identify and repair all damaged components of the phone. Evaluating the extent of the damage and whether data is recoverable from the device requires obtaining access to the device as a next step. Such access might also provide more information about the root cause of the underlying damage and when it occurred.

14. Upon instruction, my next step would be to prioritize additional attempts to repair the additional components that connect to the charging port inside the iPhone, as the charging port is critical for forensic data collection on an iPhone. This is because imaging an iPhone requires connecting a lightning connector or USB C connector to the charging port. Forensic acquisition via a wireless connection is possible with Android devices but is not currently possible with Apple devices like the iPhone at issue.

---

phone "sparking" was significant, I would expect both internal and external damage to the phone consistent "burn marks." I would also expect smoke coupled with the sparking, but Mr. Danis did not testify to seeing any smoke.

Estimated Costs

17. I estimate that the next step of conducting additional testing and procuring and installing new assemblies, parts, etc., in an attempt to replace the damaged components of the iPhone, including the charging port, would cost up to $5,000 (inclusive of parts and labor).

18. From there, if we are successful in restoring the damaged components of the phone and powering it on, assuming the data on the phone has not been deemed irretrievable, I estimate that actually extracting the data, decrypting it if necessary, and generating pertinent reports such as text messages, log files, and so forth, could range between $16,000 to $23,500, a range that depends on a number of variables including the amount of data and whether the damage to the phone impacts the ability of the data to be retrieved forensically as opposed to more manual methods (which could require significant analyst time).

I declare under penalty of perjury of the laws of the United States of America and the State of California that the foregoing is true and correct to the best of my information, knowledge, and belief.

Executed on November 19, 2024 at Los Angeles County, California.

.

Erik Rasmussen

GROBSTEIN TEEPLE

ERIK K. RASMUSSEN

Principal | JD, CISSP, MS

Areas of Expertise

Practice focus in the following key areas:

- **Cyber Risk Assessments –** Assist companies in maturing their information security programs, incident response planning and mapping security controls to frameworks like NIST, PCI or the CIS Critical Security Controls (CSCs).
- **Chief Information Security Officer (CISO) and Chief Security Officer (CSO) Advisory Services –** By serving as a virtual or consulting CISO/CSO, Mr. Rasmussen helps companies create, implement, and review information security and physical security policies and procedures, developing security elements like incident response teams and insider threat programs, assisting in transitional hiring, conduct physical security assessments and administer table top exercises and other simulations for measuring the maturity of an organization's security posture.
- **Digital Forensics and Incident Response –** Mr. Rasmussen has led hundreds of investigations into network intrusions to steal payment cards, deploy ransomware, and compromise data that is a risk to national security. Mr. Rasmussen is trained and knowledgeable about mobile forensics, server/network forensics, general computer forensics, cloud forensics and live forensics using endpoint detection tools and industry standard digital forensics software and tools.
- **Penetration Testing –** Mr. Rasmussen leads a team that conducts both internal and external penetration testing to identify vulnerabilities and to generally system security, conducts open-source intelligence gathering for testing or risk exposure, deep/dark web searches, threat intelligence sharing for testing purposes, and "red team" / "purple team" exercises.
- **Expert Witness Consulting –** Mr. Rasmussen provides expertise in both state and federal legal proceedings, as well as alternative dispute resolution venues such as AAA and JAMS, by way of authoring court declarations, being deposed on behalf of clients, preparing clients for litigation by advising on various cybersecurity matters, and professional opinion/advice on forensic investigations or regulatory frameworks. Qualified as an expert in both state court and federal court

Certifications and Licenses

- The Recreational UAS Safety Test ("TRUST") Certification, October 2024
- BSIS Firearm Permit, #2679194 (California)
- BSIS Security Guard License, #6724709 (California)
- Tactical Emergency Casualty Care for Law Enforcement and First Responders (TECC-LEO), October 2023 Certified Information Systems Security Professional (CISSP), ISC2, 2014 - Present
- Bar Member, Washington State Bar Association (WSBA), 2003 – Present

Employment History

- **Total Executive Security LLC, Los Angeles, California (2024 – present):**

- As the CEO of TES, I lead client delivery with various corporate security services, such as physical security assessments, executive protection services, and other investigative services, to include, but not limited to, surveillance and security integration services. TES also coordinates event security planning services with partner companies.

- **Grobstein Teeple LLP, Los Angeles, California (2018 – present):**

  - As the Global Head of Cybersecurity and Risk Management Solutions, I lead a professional services team of digital forensics/incident responders, risk managers and information security experts. I also manage a P&L of approximately $1.2 million with global Fortune 500 clients, non-profit organizations, educational institutions, insurance brokers and high-net worth individuals.

- **Kroll Cyber Security LLC, Los Angeles, California (2016 – 2017)**:

  - As a Managing Director, I led a team of digital forensics/incident responders, risk managers and information security experts. I also created the Payment Card Industry (PCI) program at Kroll, which included a team of PCI Forensic Investigation experts.

- **Visa Inc., Ashburn, Virginia (2014 – 2016):**

  - As a Director, I was a part of Visa's Payment System Risk team that assisted merchants is sharing cyber threat intelligence, breach identification protocols, and cyber fraud data.

- **FIS Global, Reston, Virginia (2013 – 2014):**

  - As an IT Security Manager, I assisted the internal incident response team at FIS Global, the Chief Information Security Officer, and his two Deputy Chief Information Security Officers in managing internal risk management, to include fraud incidents, employee misconduct, and data security incidents.

- **United States Secret Service, Seattle, Washington | Los Angeles, California | Washington, DC (2004 – 2013):**

  - As a Special Agent with the USSS, I conducted domestic and international computer crimes investigations and prepared federal charging documents with the Department of Justice for criminal violations related to Access Device Fraud, Bulletproof Hosting Services, Child Pornography, Distributed Denial of Service (DDoS) Attacks, Internet Relay Chat (IRC) Botnet Attacks, and Wire Fraud. From 2009 to 2011, I was a member of the Los Angeles FBI Joint Terrorism Task Force, where I conducted investigations into domestic terrorism and international terrorism.

- **Pierce County Prosecuting Attorney's Office, Tacoma, Washington (2003 – 2004):**

  - As a Deputy Prosecuting Attorney, I prosecuted both general misdemeanors and domestic violence misdemeanors and chaired 15 bench and jury trials.

- **United States Army Judge Advocate General's Corp, Fort Lewis, Washington (2001):**

- As an intern, I observed and assisted JAG officers with Legal Assistance matters, Trial Defense Service matters, as well as shadowed the JAG officer seconded to the Amy's Criminal Investigation Command (CID).

Education

- Master of Science, Leadership, The Citadel Graduate College, Charleston, SC, 2024
- Juris Doctor, Seattle University School of Law, 2003
- Bachelor of Arts, History; Departmental Honors with Distinction, Occidental College, 2000

Professional Affiliations

- Member, Georgetown University Wargaming Society, 2024 – present
- Member, Fight Club International, 2024 – present
- Member, Unites States Secret Service Association, 2024 - present
- Member, U.S. Naval Institute, 2023 - present
- Member, Institute for Critical Infrastructure Technology (ICIT), 2023 - present
- Member, California Receivers Forum, 2022
- Young Professionals Council, California Receivers Forum, 2021-2022
- Member of ASIS International, February 2018 – February 2019
- Member of Information Systems Security Association (ISSA), January 2017 – December 2017
- Member of Association of Threat Assessment Professionals, July 2016 – 2018
- Advisory Board Member, Flashpoint Partners, 2015 – 2019
- Member of International Information Systems Security Certification Consortium, Inc. (ISC2), 2014 - Present
- Washington State Bar Association (WSBA), 2003 – Present

Speaking Engagements

- Guest Speaker, Chapman University, November 2024.
- Webinar participant, CDR Case Files: Incident Response At a Law Firm (Part 1), Obsidian Security, April 2020.
- Panelist, The Exchange Data Privacy and Cybersecurity Forum, Today's General Counsel, Los Angeles, California, December 2019.
- Presenter, CyberSecure LA, Graziado Business School, Pepperdine University, October 2019.
- Panelist, The Exchange Data Privacy and Cybersecurity Forum, Today's General Counsel, Los Angeles, California, December 2018.
- Presenter, CyberSecure LA, Graziado Business School, Pepperdine University, October 2018.
- Email: Your Organization's Best Friend or Worst Enemy?, Pillsbury/Kroll Webinar, Los Angeles, California, October 2017.
- Hot Topics in Data Breach: Information Security Trends, Bradley/Kroll Webinar, Reston, Virginia, June 2016.
- "Kuhook" Point-of-Sale Malware, Visa Inc. Webinar, Ashburn, Virginia, January 2016.
- Data Breach Findings, CIO Summit, Washington, DC, December 2015.

- Breaking Cybercrime: Real-Life Case Studies from Today's Top Security Experts, Nuix Webinar, Washington, DC, October 2015.
- Game of Drones: New Breach Detection Methods, IBM i2 Summit for a Safer Planet, Washington, DC, September 2015.
- Best Practices in Cyber Threat Information Sharing, NG Security Summit, San Antonio, Texas, May 2015.
- Identifying and Mitigating Threats to E-Commerce Payment Processing, Visa Inc. Webinar, Ashburn, Virginia, March 2015.
- The Lifecycle of Cybercrime, RSA, San Francisco, February 2013.
- The Faces of Fraud: An Inside Look at the Fraudsters and Their Schemes, RSA, San Francisco, February 2012.

Training

- PFI New 2023 Fundamentals, PCI SSC, October 2023
- PFI Fundamentals Course, PCI SSC, July 2023
- *Leveraging the Intelligence Cycle*, ISC2, May 2023
- *Ransomware: Identify, Protect, Detect, Recover*, ISC2, May 2023
- *Securing the Remote Workforce*, ISC2, May 2023
- *Navigating Cyber Insurance*, ISC2, May 2023
- Payment Card Industry Qualified Security Assessor (QSA), PCI SSC, 2016 - 2018
- FS-ISAC Cyber Threat Intelligence Training, FS-ISAC, 2015
- Private Sector Overseas Security Seminar, Overseas Security Advisory Council (OSAC), 2014
- Computer Attack Methods, Central Intelligence Agency (CIA), 2012
- Prevention of and Response to Suicide Bombing Incidents (PRSBI), Department of Homeland Security (DHS), 2010
- Introduction to Networks and Computer Hardware, Defense Cyber Investigations Training Academy (DCITA), 2006
- "Point of Sale" Investigations Basics, Trustwave Holdings
- Basic Internet Investigations, Federal Bureau of Investigation
- LiveWire Network Forensics, WetStone
- Digital Forensics, Paraben Corporation
- "XNet" Pen Register Analysis, PenLink
- Critical Systems Protection Initiative, United States Secret Service
- Network Intrusion Responder Program, United States Secret Service
- Basic Investigation of Computer and Electronic Crimes Program (BICEP), United States Secret Service

Thought Leadership

- Author. "Leadership and Risk Management In IT Security: How to Guide and IT Security Team in a Complex Organization." *Today's General Counsel*, December 2022.
- Author. "The Threats of An All-Remote World." *Washington State Bar News*, July/August 2020.

Litigation Experience

- *Netlogic Solutions, Inc. v. Anil Dhondi*, In the Circuit Court for Fairfax County, 2024. (State Civil Case).

- Testified by deposition.

- *Tin Packing Ltd. et al. v. Kang Li et al*. Middle District of Tennessee, 2024. (Federal Civil Case).
- *State of California v. Galina Migalko and Robert Young*, Superior Court of the State of California, 2024 (State Criminal Case).
  - Testified in motion hearing.
- *Netlogic Solutions, Inc. v. ZoleyTech, Inc.,* American Arbitration Association, 2023 (Arbitration).
  - Expert testimony.
- *Olivine, Inc. v. Zero Net Energy Alliance, Inc. et al.*, Superior Court for the State of California, Yolo County, 2023 (State Civil Case).
- *Lindabeth Rivera, et al. v. Google, LLC*, Cook County Chancery Division, 2023 (State Civil Case).
- *John Doe v. Serbian Orthodox Diocese of Western America*, Superior Court for the State of California, Los Angeles, 2022 (State Civil Case).
- *In the Matter of: First American Title Insurance Company, Respondent*, New York State Department of Financial Services, 2021 (State Civil Case).
- *In Re: Marriott International Customer Data Security Breach Litigation*, District of Maryland, Southern Division, 2021 (Federal Civil Case).
  - Testified by deposition.
- *Honor Finance, LLC, Honor Finance Holdings, LLC v. Spireon, Inc*., Superior Court of the State of California, County of Orange, 2021 (State Civil Case).
- *CMZ of Hawaii, Inc. v. Pacific Foundation, Inc.,* District of Hawai'i, 2021 (Federal Civil Case).
  - Testified by deposition.
- *People v. Kailin Wang*, Superior Court of California County of San Francisco, 2021 (State Criminal Case).
- *United States v. Joshua Thomas Bales*, Western District of Washington, 2021 (Federal Criminal Case).
- *Emmalee Forrester et al v. Clarenceville School District et al*, Eastern District of Michigan, 2020 (Federal Civil Case).
- *Rachel Sims v. Little Rock Plastic Surgery P.A.*, Eastern District of Arkansas, 2020 (Federal Civil Case).
- *Iacovacci v. Brevet Holdings et al*, Southern District of New York, 2020 (Federal Civil Case).
  - Testified by deposition.
- *Quid, Inc. v. Primer Technology, Inc. et al*, Superior Court for the State of California, San Francisco, 2020 (Arbitration).
  - Testified by deposition.
- *Danford v. Lowes*, Western District of North Carolina, 2019 (Federal Civil Case).
- *Mitchell v. Marketing Corporation of America d/b/a Fine Art Models*, St. Clair County Circuit Court, Michigan (State Civil Case).
  - Testified at trial.
- *Thygesen v. Wang*, Superior Court for the State of California, San Francisco, 2019 (State Family Law Case).
- *In re Jonathan Edward Anderson and Amanda Marie Anderson / Jeremy W. Faith, Chapter 7 Trustee, Plaintiff v. Samantha L. Caron and James S. Caron*, Central District of California, 2019 (Federal Bankruptcy Case).
- *Waldbaum v. Slodzinski, et al.* Circuit Court of Maryland, Baltimore City, 2019 (State Civil Case).
- *Laughlin v. Sinai Hospital*, Circuit Court of Maryland, Baltimore City, 2018 (State Civil Case).
- *Chelsea Hamilton v. Wal-Mart Stores, Inc. et al,* Central District of California, 2018 (Federal Civil Case).
- *Ortolani v. Freedom Mortgage Corporation*, Central District of California, 2018 (Federal Civil Case).
- *KCG Holdings v. Rohit Khandekar,* Southern District of New York, 2017 (Federal Civil Case).
  - Testified by deposition.

GROBSTEIN TEEPLE

- *Alexis v. Rogers*, District Court for Southern California, 2017 (Federal Civil Case).
- *United States v. Sergey Vovnenko*, District of New Jersey, 2013 (Federal Criminal Case).
- *United States v. Andriy Derkach*, Eastern District of Virginia, 2012 (Federal Criminal Case).
    - Testified at federal grand jury proceeding.
- *United States v. Robert Bentley*, Northern District of Florida, 2007 (Federal Criminal Case).
    - Testified at federal grand jury proceeding.
- *United States v. Marcus McGrath*, Central District of California, 2007 (Federal Criminal Case).
    - Testified at federal grand jury proceeding.

*Multiple jury trials, court appearances and motion hearings as a Deputy Prosecuting Attorney

Examples of Experience

- Virtual CISO support for humanoid robotics AI firm with almost a $3 billion valuation.
- Virtual CISO support for insurance brokerage firms, nonprofits, international ticket brokerages, AmLaw 100 law firms, and various small businesses.
- Digital forensics incident response support for multiple ransomware attacks, to include the following ransomware families: Conti, Hive, Locky, and Zeppelin.
- Digital forensics incident response support for multiple victims of “Business Email Compromise” attacks.
- Digital forensics incident response support for national restaurant groups, municipalities, real estate companies, and various other entities suffering from ransomware attacks, Magento e-commerce attacks, and other suspected or actual network intrusions.
- Digital forensics support and forensic accounting assistance for a Los Angeles-based radio station in an internal investigation into fraud and embezzlement.
- Digital forensics support in the automotive industry in *Schrage v. Schrage*, a receivership matter for Sage Automotive Group that has required the forensic acquisition of dozens of systems, cyber risk assessment work, and specialized forensic analysis of legacy IBM systems.
- Ongoing cyber risk assessment support, mobile forensics support and computer forensics support for a regional aerospace firm.
- CISO support to a global e-discovery firm, insurance brokerages, a medical facility, a global non-profit, and various hospitality and law firm clients.
- Led numerous engagements or provided court declarations in which employees were accused of siphoning sensitive company data via both digital methods, such as cloud-based services, and through physical means, such as surreptitiously photographing financial data for use by a criminal organization.
- Led or oversaw offerings of governance and risk assessments for global retailers, e-commerce companies, nonprofit organizations, Presidential libraries, educational institutions and various aviation and defense contractors.
- Managed several international payment card breaches and assisted in the arrest of transnational targets of enterprise level data breaches.

GROBSTEIN TEEPLE

- Provided expert testimony for medical center breaches in litigation, and counseled insurance companies dealing with insider threats, billionaire fund managers addressing online and email cyber threats, and theft of trade secrets.
- Led or trained global asset management firms, payment processors in interviewing techniques, and Interpol for cyber fraud trends.
- Provided security support for private wealth management firms, global supply chain companies, celebrities and other high net worth entities or individuals that have either experienced an incident or seek improvement in their internal security capabilities.